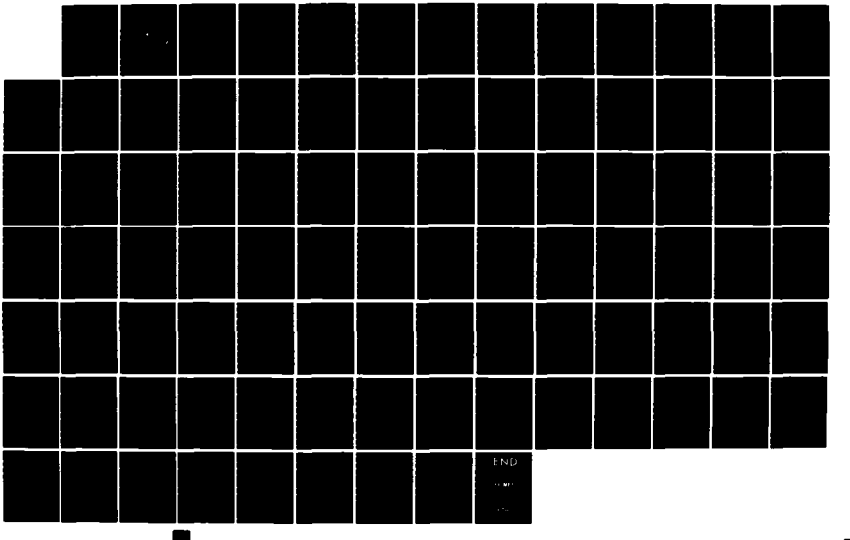
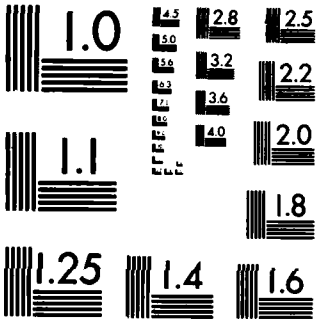
AD-A155 536 SECURITY CONTROLS IN THE STOCKPOINT LOGISTICS INTEGRATED COMMUNICATIONS ENVIRONMENT (SPLICE)(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA D S ARSENEAULT MAR 85 1/1

UNCLASSIFIED F/G 9/2 NL





NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

SECURITY CONTROLS IN THE STOCKPOINT LOGISTICS INTEGRATED COMMUNICATIONS ENVIRONMENT (SPLICE)

by

Daniel Scott Arseneault

March 1985

Thesis Advisor: Norman F. Schneidewind

Approved for public release; distribution is unlimited

unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A153 536	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Security Controls in the Stockpoint Logistics Integrated Communications Environment (SPLICE)		5. TYPE OF REPORT & PERIOD COVERED Master's Thesis March 1985
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Daniel Scott Arseneault		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93943		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, California 93943		12. REPORT DATE March 1985
		13. NUMBER OF PAGES 89
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

computer security, stock points, logistics, computer systems, ... SPLICE

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This thesis examines security controls specified and implemented in the Stock Point Logistics Integrated Communications Environment (SPLICE) project. Controls provided by the Defense Data Network and the Tandem operating system are reviewed. Alternatives from current literature in areas of authentication, encryption, and dial-port protection are

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE S/N 0102-LF-014-6601

unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

reviewed for the purpose of suggesting enhancements. Issues discussed apply to most interactive/decentralized systems in operation today and include administrative as well as technical recommendations.

Approved for public release; distribution unlimited.

Security Controls in the Stockpoint Logistics Integrated Communications Environment (SPLICE)

by

Daniel Scott Arseneault
Lieutenant, United States Navy
B.S., Georgia State University, 1976

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
March 1985

Author: Daniel Scott Arseneault
Daniel Scott Arseneault

Approved by: Norman F. Schneidewind
Norman F. Schneidewind, Thesis Advisor

Norman R. Lyons
Norman R. Lyons, Second Reader

Willis R. Greer, Jr., Chairman,
Department of Administrative Sciences

Kneale T. Marshall
Kneale T. Marshall,
Dean of Information and Policy Sciences

ABSTRACT

This thesis examines security controls specified and implemented in the Stock Point Logistics Integrated Communications Environment (SPLICE) project. Controls provided by the Defense Data Network and the Tandem operating system are reviewed. Alternatives from current literature in areas of authentication, encryption, and dial-port protection are reviewed for the purpose of suggesting enhancements. Issues discussed apply to most interactive/decentralized systems in operation today and include administrative as well as technical recommendations.

TABLE OF CONTENTS

I. INTRODUCTION ---------- 10

II. DEVELOPING SECURITY FOR COMPUTER SYSTEMS ------ 11

A. SYSTEM EVOLUTION CREATES NEW VULNERABILITIES 11

B. FEDERAL REQUIREMENTS FOR SECURITY SPECIFICATION ---------- 12

C. WHY DELIVERED SYSTEMS DON'T MEASURE UP? --- 13

D. RECOMMENDATIONS FOR IMPROVEMENT ---------- 17

E. HOW MUCH SECURITY IS ENOUGH? ---------- 20

III. THE SPLICE SYSTEM ---------- 24

A. BACKGROUND ---------- 24

B. THE SECURITY ISSUES ---------- 28

C. SYSTEM SCOPE ---------- 28

D. CURRENT TOPOLOGY ---------- 29

E. IMPLEMENTATION ISSUES ---------- 31

F. SITE SECURITY ---------- 32

G. SPLICE DATA ---------- 33

IV. THE IMPACT OF DDN ON SPLICE SECURITY REQUIREMENTS ---------- 34

A. DDN, THE NETWORK TO BE UTILIZED ---------- 34

B. DDN, ORIGINAL TOPOLOGY ---------- 35

C. DDN, ACTUAL EVOLUTION ---------- 35

D. DDN, ENCRYPTION ---------- 36

E. PHYSICAL SITE, PERSONNEL ---------- 38

F. ELECTRICAL EMMISIONS ---------- 38

G. ACCESS, ROUTING, DELIVERY ---------- 38

H. THE SPLICE RESPONSE ---------- 39

V. SECURITY CONTROLS IN SPLICE ---------- 41

A. SPECIFICATION ---------- 41

B. COMPONENT DEVELOPMENT ---------- 43

C. SAS OPERATIONS ---------- 49

D. LEVEL OF SECURITY PROVIDED ---------- 51

VI. SURVEY OF AUTHENTICATION ---------- 52

A. REASONS FOR AUTHENTICATION ---------- 52

B. WHAT CAN BE USED TO AUTHENTICATE? --------- 53

C. SOMETHING A PERSON KNOWS ---------- 53

D. SOMETHING A PERSON HAS ---------- 56

E. SOMETHING A PERSON IS ---------- 57

F. DOES SPLICE AUTHENTICATION SUFFER? -------- 62

VII. ISSUES IN FILE AND TRANSMISSION PROTECTION ---- 63

A. WHAT IS ENCRYPTION? ---------- 63

B. ATTACKS ON DATA ---------- 64

C. WHAT SHOULD BE ENCRYPTED? ---------- 65

D. WHEN SHOULD ENCRYPTION BE EMPLOYED? ------- 66

E. THE COSTS OF ENCRYPTION ---------- 67

F. ENCRYPTION METHODS ---------- 70

G. PORT PROTECTION ---------- 71

VIII. CONCLUSIONS/RECOMMENDATIONS ---------- 76

A. CONCLUSIONS ---------- 76

B. RECOMMENDATIONS ---------- 77

APPENDIX A ---------- 80

LIST OF REFERENCES ---------- 82

BIBLIOGRAPHY ---------- 86

INITIAL DISTRIBUTION LIST ---------- 89

LIST OF FIGURES

		Page
3.1	Local SPLICE Site Topology	27
3.2	SPLICENET	30
4.1	Unclassified Segment of DDN	37
5.1	SAS Context Diagram	44
5.2	SPLICE System Logical Flow	46

LIST OF TABLES

		Page
3.1	Hardware Systems in SPLICE	25
7.1	Data Encryption Sampler	68
7.2	Dial-up Port Protection Devices	75

I. INTRODUCTION

This thesis examines technical and to a limited extent, administrative security controls implemented in the Stock Point Logistics Integrated Communications Environment (SPLICE). Not all controls included in SPLICE systems are discussed; the purpose of this thesis is identification of those areas where improvements seem warranted. Following a brief discussion of general security issues, SPLICE, the Defense Data Network (DDN), and SPLICE security systems will be reviewed. I will then cover alternative authentication, encryption, and dial-up port protection techniques from current literature and conclude with recommendations for follow on activities.

The information contained in this thesis was gathered during interviews with personnel at Naval Supply Center Oakland and a review of the literature referenced. All references to specific software packages, authentication devices and encryption/dial-port products are taken from sources identified without attempts to compare claimed capabilities and should be taken only as an example of products available and not the last word in that area.

II. DEVELOPING SECURITY FOR COMPUTER SYSTEMS

A. SYSTEM EVOLUTION CREATES NEW VULNERABILITIES

As systems develop allowing individual access by a user to computer resources, the potential for data loss or compromise increases dramatically. Users are discovering advantages in real-time response and are creating requirements for such applications.

In traditional batch processing environments, user access to system resources was limited to the few data processing personnel responsible for loading and operating the system. These systems were typically centralized and physically located in one building, often in one room. Security was often assured only by guarded or locked doors. As users have gained control of resources the resources have migrated out of the physically secure data center to the user workplace.

During this same period of time, geographically dispersed elements of large organizations recognized a real-time need to pass not only bulk files but also short unstructured inquiries. As a result, data communications requirements grew rapidly.

The Navy's largest logistics system, the Uniform Automated Data Processing System-Stock Points (UADPS-SP),

was one organization affected by this proliferation of both interactive and data transmission applications.

As an organization's data processing resources spread out two problems come to the surface immediately:

1) How can the central processing site ensure that only authorized users access processes or files?

2) How can the organization protect data during transmission?

While these vulnerabilities existed to a limited extent in the previous system they must now receive more attention.

B. FEDERAL REQUIREMENTS FOR SECURITY SPECIFICATION

In 1978 the Office of Management and Budget issued Circular A-71 [Ref. 1] requiring security specifications in all new Automatic Data Processing (ADP) developments and procurements. The Department of Defense (DOD) and the Navy have since updated their own instructions regarding ADP security, to include a requirement for Activity ADP Security Programs, risk analysis and accreditation of acceptable protection prior to system operation [Ref. 2].

To date, the major security improvements made in the field appear strongly influenced by the development of such tools as threat, safeguard, compliance, and certification checklists. A problem that has resulted is the development of these checklists by individual activities for internal use without efforts for sharing across the organization. The principal reason for this appears to be the result of

instructions specifying "activity" level responsibility [Ref. 2]. Large geographically dispersed projects like SPLICE will require more organizational direction regarding security due to the many connections between activities. It would appear common procedures among SPLICE activities would help.

C. WHY DELIVERED SYSTEMS DO NOT MEASURE UP?

Computer systems continue to arrive at activities with significant gaps in security controls apparent. These systems were apparently developed without a full understanding of organizational requirements. [Ref. 3]

Threats were never recognized by activities because activities do not take time to think about things that only "might" happen. "Too often, the question of data destruction or misappropriation goes unanswered until a disaster occurs." [Ref. 4: p. 17]

Persons responsible for conducting a "Risk Analysis" were possibly not experienced or did not take the time to properly review potential problem areas due to the "press of business". In the insurance industry, a need for insurance should be established and the value of having a policy quantified and compared to its cost. Security safeguards are a form of insurance. Loss equates to what the organization will give up should its data be compromised or destroyed. Risk combines loss with probabilities that the

threat will be realized. While high risk demands higher security, without some form of quantification managers will not know where to spend money on safeguards. Unfortunately the largest threat and the one threat most systems tend to ignore is posed by authorized users in systems lacking effective audit trails [Ref. 5: p. 62].

Data value has not been quantified. Organizations that have not taken or were not given the time to hierarchically organize their data by value and potential for compromise are finding it difficult to select appropriate safeguards [Ref. 6].

Specifications do not fit requirements. Rather than analyze their own activities, the user's specifications are often developed only to those minimally required in written instructions. The resulting systems are based on the vendor's determination of security needs utilizing only those specifications. These systems require expensive add-on features, often causing more problems than they alleviate. While many might argue that "non-specific" specifications enable faster delivery, lower cost, and increased industry participation the result can be disappointing.

Some organizations opt for a system meeting only end-result processing requirements under perfect operating conditions. One error or omission in input may bring the operation to a standstill. Organizations not specific in

making system security needs known leave security to the discretion of the software designer. Since software focus is on a comprehensive, efficient product, and security often cuts into efficiency, designers tend toward the minimum [Ref. 7].

An organization can also overspecify. If an organization does not have the expertise to realize the constraints their specifications will have on operations, the result can be disaster. If every part of the system is treated as critical without regard to risk or data value the resulting product may be so slow that meaningful work cannot be done. Overspecification can lead an organization into believing their system to be invincible. This has been termed the "Maginot Line Syndrome" [Ref. 8: p. 51]. This may also result in neglect of other important administrative controls.

Personnel providing specifications often do not have computer security expertise. Many activities have been caught short by regulations requiring responsibility for security to be vested in an official familiar with both ADP and security [Ref. 1: p.3]. Personnel are often assigned who are familiar with ADP or security but not both. Security personnel often are not computer security personnel. Many of our colleges and universities do not offer courses dealing specifically with this subject and it

appears general security expertise among ADP personnel is suffering. Many activities do not pay individuals in this position the salary they may draw elsewhere for their computer experience alone.

Another problem results from reliance on military officers for the security function. On arrival they have little or no experience; just when that experience is developed they transfer. An activity's security function deserves continuity.

Personnel reviewing/approving specifications often have erroneous perceptions of security. Many users and managers consider security a dirty word.

> "When enhanced security is mentioned, many people immediately equate this to reduced capability, less friendly operations, and restrictive personnel practices." [Ref. 9: p. 93]

Most controls are resented: slowing users down; adding to costs; and frequently not essential for work being done [Ref. 10: p. 9]. It is those few applications needing protection that must be brought in focus. Due to past experience or "gut feelings", many security features have been summarily cut from systems before development only to be recognized during implementation or operation as critical. Adding security then would likely be more expensive and create a system that may not operate within the user response requirements for which it was built. A danger exists that the weakness just might be ignored.

D. RECOMMENDATIONS FOR IMPROVEMENT

To improve the overall security posture of any activity all the above problems must be addressed simultaneously. Qualified personnel providing effective specifications may not overcome management bias. Adequate risk analysis won't overpower poor safeguard specification or selection. The organization must take a balanced approach to developing corporate knowledge of security as well as security controls. An NBS workshop on audit and security in 1978 concluded that security policy must be set and security mechanisms must be put in place and be constantly evaluated to assure effectiveness [Ref. 11: p. 56].

Threat recognition takes time and creativity. An organization should identify common threats and leave only identification of specific activity threats to the activity. Besides published threat checklists, a valuable technique is development of threat scenarios and analysis of their impact on the activity. The scenario approach alone has been found lacking in DOD attempts to ensure systems security by detailing "Tiger Teams" to attempt penetration; later checks of the system showed the Teams often left significant vulnerabilities untested or the fix prescribed resulted in new vulnerabilities [Ref. 11: p. 56]. Threats should not be immediately dismissed out of hand. Threat assessment is a challenge. This is a process where many creative

individuals should be involved; do not rely on the ideas of one person.

Once threats are recognized their probability of occurence should be judged. Since historical data most likely is lacking here this judgement should be biased toward their actual occurrence for an extra measure of protection.

The loss value of data which would be compromised or destroyed should the threat be realized must be computed. Excellent suggestions regarding threat recognition/probability and loss determination have already been made for SPLICE [Ref. 12: p. 24-63].

An excellent aid to identifying valued data resources is the "Data Dictionary/Directory". Such a tool defines each entity, its use, and its relationships and has been proposed for SPLICE [Ref. 13]. Involvement in constructing a data dictionary/directory for the activity ensures that both user and designer will inspect usefulness of current data and consider future requirements. The result will be a firm base from which to select safeguards or specific security features. Such aids can also assist in standardization between sites.

Specifications must be improved. Current systems appear to be placing too much emphasis on getting products to the workplace with the idea of leaving the patching of security to implementation and operational personnel. Lack of

specification detail convinces top management the safeguard is unimportant.

Personnel involved in organizational security must be qualified. If none are currently on board the organization should seek professional outside assistance. This should only be a temporary fix, organizations should rely on outsiders for security only as a last resort. If expertise cannot be found in the local labor market, internally generated talent should be drawn on. Organizational security requires continuity, therefore I would recommend all security departments have more than one individual familiar with requirements and procedures. On the other hand, security safeguard specifics should be known to as few individuals as possible to prevent employee attempts at circumventing the system. Security manuals and specific documentation should be kept out of general circulation.

Perceptions of security must be "adjusted" to conform to system security needs. Both users and management must be educated to view security as a "business" problem [Ref. 14: p. 7]. Issues must be described to them in common business terms [Ref. 4: p. 22]. Data must be viewed as an asset. It will be difficult to convince users of security importance if top management is openly cold toward it. The security department's first goal should thus be top management support. Without authority from above the security

department's chance for successful system security is greatly diminished, even if technical safeguards are in place.

"Management sets the moral climate of a company" [Ref. 15: p. 32] if upper level managers view security safeguards and procedures as unimportant or not applicable to them, and if security is openly ignored, users will exhibit similiar attitudes and behavior.

Users and management must be shown examples of successful system approaches to security instead of the inefficiency introduced by some add-on features. A source of examples may be found in the recently created DOD Computer Security Center's Evaluated Products List [Ref. 9: p. 94]. The DOD Computer Security Center has additionally put together the DOD Trusted Computer Systems Evaluation Criteria to assist in organizational security development [Ref. 11: p. 57].

E. HOW MUCH SECURITY IS ENOUGH?

How secure any system actually is cannot be quantified in any but relative terms and is based on both the environment and security safeguards in place. No safeguard or combination of safeguards can guarantee 100% that data is safe in a system. Any attempt to even approach this figure utilizing present technology almost ensures that a system cannot be used. At the other extreme, the most user

friendly system would exhibit great vulnerabilities. What every system security policy should ensure is a balance of these two traits to a degree commensurate with the value of data to be protected and system risks.

The private sector has not developed any ranking for system security. The Department of Defense (DOD) has begun classifying systems by security level but as yet have not reviewed any systems meeting all criteria for one level and no others. The question of how much security a system should provide is still answered subjectively. Recent trends toward a more rigorous approach at performing Risk Assessments and selection of safeguards indicate that future formal policies may soon be established. There are as many opinions in the security industry of what constitutes adequate security as there are products. "Enough" is a matter of judgement, the judge being those who must eventually pay the price of security controls or take the risk of not applying them.

One method for specifying how much security to provide for a system is the "Prudent Person Rule" [Ref. 8: p. 171]. The "person" is that individual given responsibility for an organization's security. "Prudent" refers to his selection of the same safeguards in use by "most" of the other organizations in that industry. Supposedly, a loss occuring after such safeguards are in place would not be blamed on the prudent person but would instead be marked off as

unavoidable. Organizations operating under this technique need do little in the way of risk assessment as management probably will not approve any controls their contemporaries have not first embraced.

Another view of how much security is enough centers on the assumption that the potential penetrator is a "reasonable man" and would not spend more on obtaining data then could be derived from it [Ref. 8: p. 53]. Here data value is "specifically" derived (a judgement call) and security controls are increased only to that point where the "reasonable man" would give up attempts at access (a judgement call). This technique too has a drawback, data of low value to an outsider may be critical to an organization's continued health and needs protection from accidental or malicious destruction.

For most day-to-day users of a system, "enough" is whatever allows one to get a job done in peace. Many users would probably consider no controls adequate; it is thus the responsibility of management to ensure that the user knows what this could mean. While user opinions may be valuable in defining just what interface a security control should assume they should not be relied on to pass judgement on the appropriateness of specific controls.

No one criteria should be relied on in determining the degree of security to employ, instead, it appears the best

policy is to combine attributes of all. First it is essential data value be somehow determined; value, not only to an outsider, but to the firm's operation. Next, all potential safeguards both physical and administrative should be identified and costed out. There is nothing wrong with reviewing what other organizations are doing (if the information is available) so long as innovative approaches are not ruled out.

"No single control can stop - or deter - the computer criminal" [Ref. 16: p. 21]. A series of "package deals" should be prepared so that top management decisions for a system will be based on a system and not just a list of safeguards.

It has also been suggested that security be added one piece at a time where systems managers have previously balked at a comprehensive package [Ref. 14: p. 13]. While this flys in the face of advocating built-in security, it may be the only way security will be provided for a system that already exists.

III. THE SPLICE SYSTEM

A. BACKGROUND

In late 1977 the Naval Supply Systems Command formally recognized a need for data communications and processing support for the Burroughs medium computer systems of the UADPS-SP [Ref. 17: p. 3-1]. This system handles the bulk of U.S. Navy logistics community ADP requirements. A rapid growth in both number and type of computer applications requiring an interface with the files maintained in UADPS-SP Systems was occuring and was projected to accelerate. Many of these applications were of a real-time interactive nature. Many were running on other computer systems; some long distances away from the UADPS-SP sites. The Burroughs equipment, developed to operate in a batch environment, was rapidly being saturated with these multitudes of interactive processes and communications handling requirements [Ref. 18: p. 2-2].

Computer compatibility had become a big problem. Even at the same geographical location, different users in the logistics community had developed systems with components from a variety of manufacturers. Examples of major hardware systems currently utilized in the various logistics communities to be tied together by SPLICE are noted in Table 3.1.

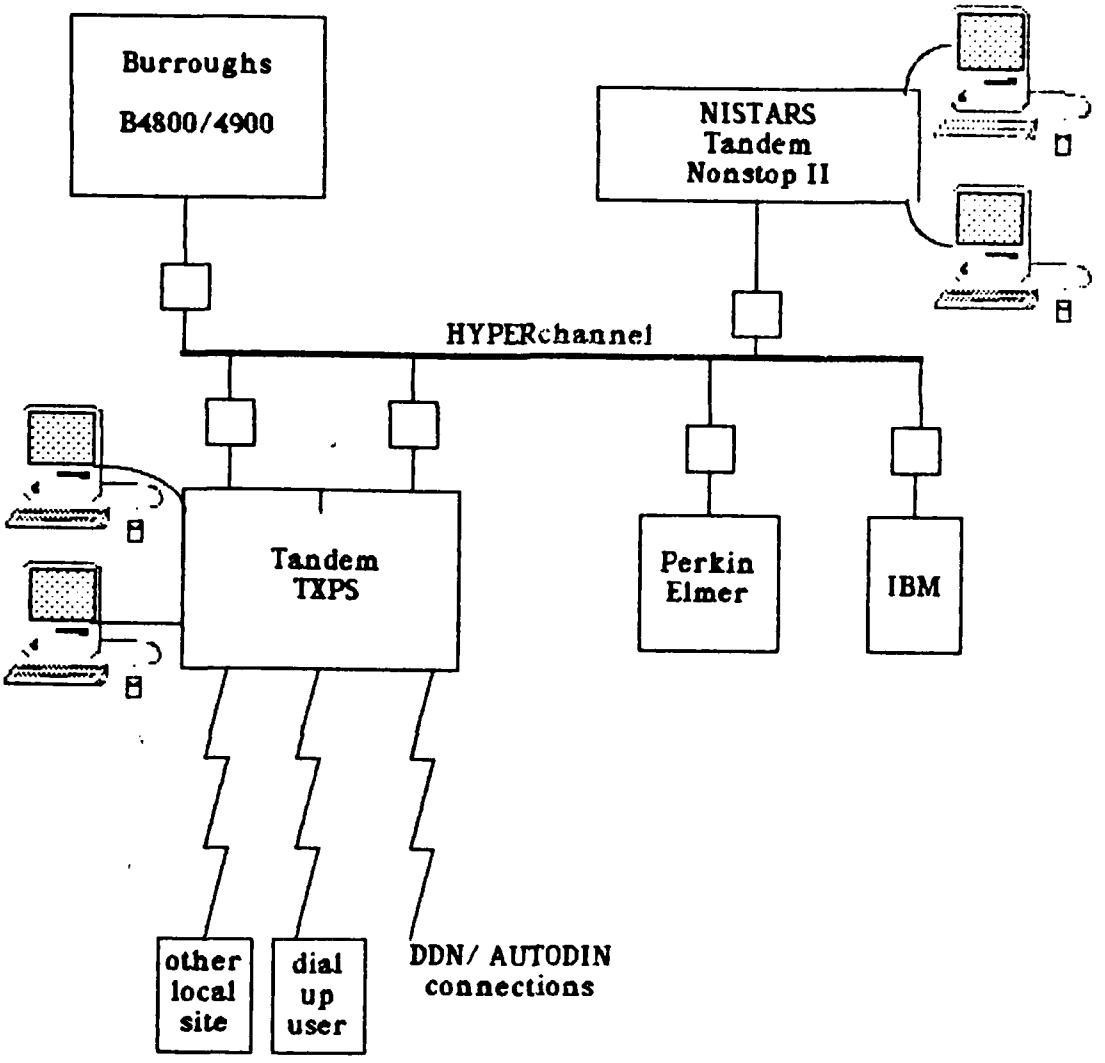
Table 3.1

Activity/Application	Computers
Defense Automatic Addressing System (DAAS)	CDC 3500
Defense Logistics Agency Network (DLANET)	Comten 36xx
Automation of Procurement and Accounting Data Entry (APADE)	P-E 3200
Navy Integrated Storage Tracking and Retrieval (NISTARS)	Tandem Nonstop II
Multiple Activity Processing System (MAPS)	B 1700/1800/1900 Mohawk 2400 Nova 800 I/D 7-32 P-E 3200
Uniform Automated Data Processing System (UADPS-SP)	B4800/4900
Integrated Disbursing and Accounting (IDA)	P-E 3230 Univac 1100
Inventory Control Point Network (ICPNET)	IBM
Naval Automated Transporation Documentation System (NAVADS)	P-E 3200

[Ref. 18: p. 2-7]

These same logistics communities developed their own local and long distance data communications networks operating on a variety of protocols. Many of the interconnections that were developing came as the result of specific user initiative rather than any formal plan for future connectivity. [Ref. 18: p. 2-3]

The SPLICE concept centers around a standard hardware/software suite of minicomputers to be placed at each logistics site. A common communications medium would be chosen to interconnect all sites. Adaptive interfaces would be developed to interconnect all the various systems in a site's geographical area and enable their use of this one network. SPLICE equipment and software was to provide a failsafe fail/soft processing environment [Ref. 18: p. 2-5]. The SPLICE minicomputer would be tasked with processing interactive applications and acting as a communications front-end for the Burroughs. Video terminals would replace keypunch entry. The Burroughs would be freed to handle large file processing and reporting functions for which it was originally intended. Eventual replacement of the UADPS-SP hardware was to be eased by the flexibility SPLICE would provide in opening selection to a wider range of ADP equipment. [Ref. 17: p. 1-5] Figure 3.1 illustrates a typical SPLICE site configuration.



Local SPLICE Topology

Figure 3.1

B. THE SECURITY ISSUES

The various systems to be interconnected by SPLICE had been developed independently with few technical security controls imposed. Often, the locked door of their respective environments and minimal password access controls were apparently seen as sufficient. Some local systems in the recent past employed but one password for all users. Others lacked provisions for blanking out screen echo of passwords on login. SPLICE is lightyears ahead of these systems.

I see the security problem confronting SPLICE as fourfold:

1) how can users be identified to the system and will the system be able to verify their identity;

2) how can users be kept from processes and data to which they are not entitled;

3) how can data transmissions between sites be protected;

4) how can the system be monitored to ensure that violations are not occuring.

Splice is to secure access at the terminal, user, and transaction level [Ref. 18: p. 2-10]. How effectively it does this remains to be seen.

C. SYSTEM SCOPE

SPLICE is targeted for 62 separate sites in the U.S. and Pacific. At least two TANDEM processors will be in place at each. [Ref. 18: p. 3-3] Capabilities to be supported include:

"* Inventory Control Point transfer of (bulk) data files to

-another Inventory Control Point Inquiry,
-a Stock Point
-the Defense Automatic Addressing System (DAAS);

* Contingency processing between the Inventory Control Points;

* Inventory Control Point Inquiry to the data bases at
-another Inventory Control Point
-a Stock Point, and
-the Defense Logistics Agency (DLA) centers;

* Stock Point transfer of (bulk) data files to
-another Stock Point,
-an Inventory Control Point, and
-the Defense Automatice Addressing System (DAAS);

* Contingency processing capability between Stock Points;

* Stock Point inquiry to the data bases at
-another Stock Point,
-an Inventory Control Point,
-the Defense Logistics Agency (DLA) centers;

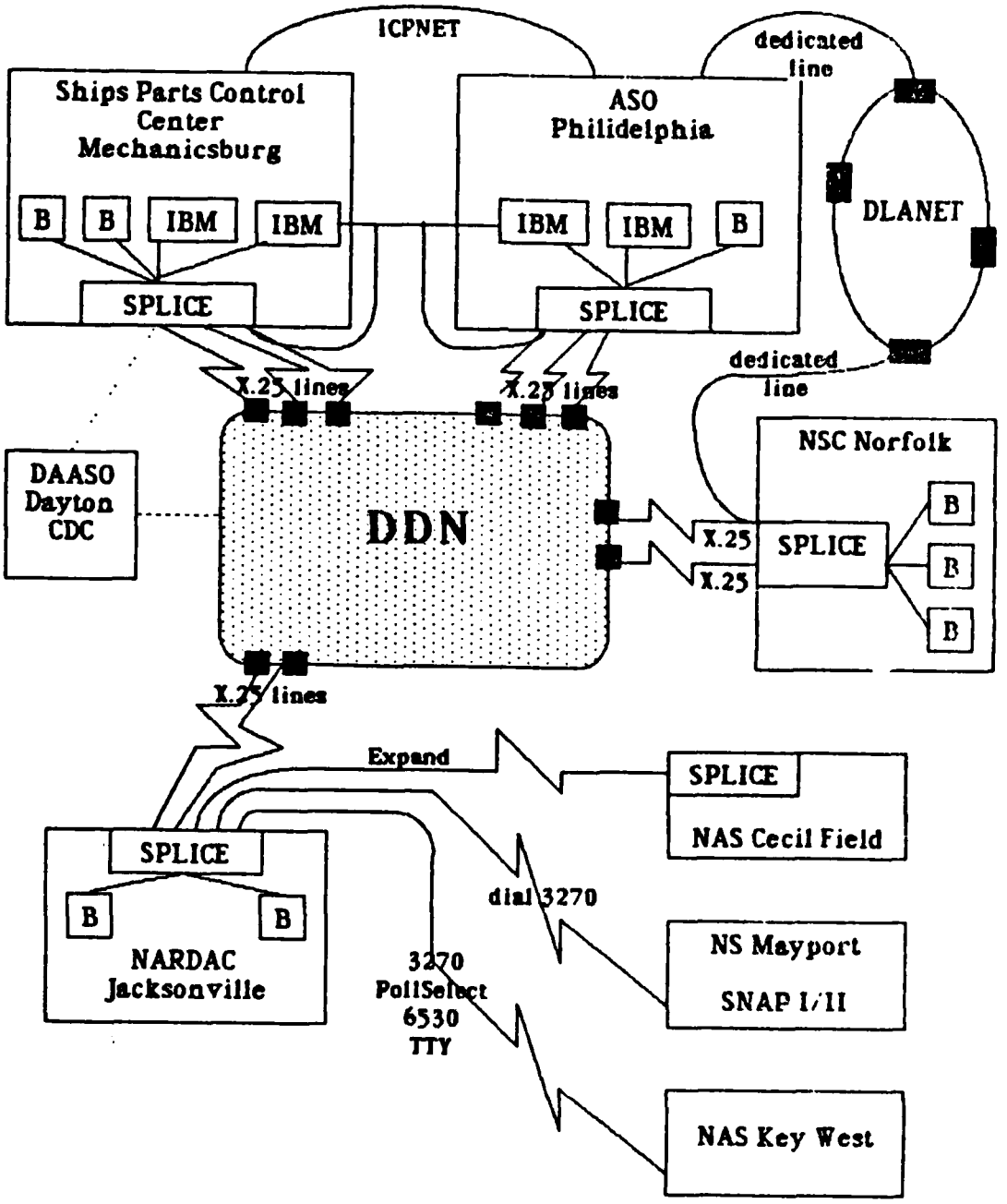
* Users from outside of the Stock Point and Inventory Control Point communities require inquiry capability into the data bases of Inventory Control Points and/or DLA centers."

[Ref. 17: p. 1-13].

If required the system will link logisitics organizations with other components in DOD folowing development of appropriate Defense Data Network (DDN) Protocols [Ref. 19: p. 8-1]. Figure 3.2 illustrates SPLICE system connections.

D. CURRENT TOPOLOGY

SPLICE contracts were awarded to the Federal Data Corporation (FDC). SPLICE is being developed on the Tandem Corporation's TANDEM TXP computers and related peripherals.



SPLICENET [Ref. 17 : p. 1-15]

Figure 3.2

Software to be utilized in the TANDEM operating system is a combination of native Tandem products (i.e. GUARDIAN, ENCOMPASS, EXPAND) and customized modules (i.e. Security Access System (SAS), System Monitor (SMON)). SPLICE sites will communicate with each other over DDN I in a closed community mode utilizing the X.25 protocol. The SPLICENET is to eventually go to a full DDN suite of protocols to enable interconnection with other users. SPLICE sites will communicate with other logisitics communities over a variety of dial-up and dedicated circuits. SPLICE computers will connect with their local community of users via NETEX software and Network System Corporation's HYPERchannel, a system of microprocessor-based adaptors and coaxial cable enabling computers from various manufacturers to communicate at high speed. [Ref. 17: Chap. 5]

E. IMPLEMENTATION ISSUES

Smooth transition to a standard communications environment will be hampered by some of the same policies being used to lower processing conversion risks. SPLICE will be implemented over a period of years. Many interim communications connections will be made and maintained during this period. In a system such as SPLICE, where risk quantification is difficult, justification for expensive technical security countermeasures for these "interim" connections will be hard to sell.

The number and variety of connections will also present a problem for control of access. Identification and maintenance of appropriate access authorization lists will be difficult. An excellent ADP security plan at one installation will not prevent unauthorized access from other sites where security is compromised. Many terminal sites will not be receiving the upgraded security features in the TANDEM system for several years. Finally, other logistics communities are not moving rapidly toward DDN implementation and their own networks may remain in place for sometime. [Ref. 19]

F. SITE SECURITY

As SPLICE is implemented at each site most of the existing terminal equipment, controllers, and peripherals are to be phased out or connected directly to the TANDEM. Only equipment tied to the TANDEM will be covered under its security access management process in SAS. Terminals remaining on the Burroughs and other local systems will continue to have their own capabilities but will not have authority to order processing by the TANDEM or access other sites [Ref. 17 p. 1-4]. Physical and administrative security controls will be unique to each site. Except for SAS passwords, few other technical countermeasures are currently in use, probably due to a lack of empirical data for justifying them.

G. SPLICE DATA

Data processed within the UADPS-SP system that will be transmitted between sites is at most sensitive business data. Individual applications within sites include inventory control, ordering, payroll, and contract administration. While administrative separation of duties ensures that little would be of benefit to an individual employee, a conspiracy could develop to profit from data manipulation. Additionally, individuals with access to a terminal could cause considerable damage to programs and files if access is not controlled to those specific objects.

The last attempt at Security Risk Assessment formally made on the system level for SPLICE appears to have been made in 1980 [Ref. 20]. Appropriate risk analysis and file value quantification are still not available. The integrity of this data is important in accounting for millions of dollars in supply transactions within UADPS-SP. Some of the data is critical for day to day operations, some is not. Since many controls are not appropriate for every system, they need to be chosen taking value into consideration. It would seem that a system wide data value quantification effort is needed so each site is using the same figures in activity security plans.

IV. THE IMPACT OF DDN ON SPLICE SECURITY REQUIREMENTS

A. DDN, THE NETWORK TO BE UTILIZED

The Defense Data Network (DDN) is an evolving data telecommunications network utilizing packet switching and slated to eventually handle most Department of Defense (DOD) long haul data transmission requirements for both classified and unclassified user communities. Many heterogeneous systems can effectively communicate with each other using a DOD standard Transmission Control Protocol (TCP) and Internet Protocol (IP); systems utilizing an X.25 protocol will be supported only until DOD standards are developed [Ref. 21: p. 2/3]. DDN I developed out of a 1981 evaluation of the Automatic Digital Network (AUTODIN II) versus the Advanced Research Projects Agency Network (ARPANET) technologies. The ARPANET technologies were chosen as a basis for DDN in April 1982. Subsequent DOD policy decisions require all DOD users, having a long haul data transmission requirement to register as subscribers with the DDN and begin development of appropriate interfaces [Ref. 22]. Decisions would be made on which activities were to be granted a waiver. SPLICE was required to subscribe and use DDN.

B. DDN, ORIGINAL TOPOLOGY

Initially, DDN was to be a network of switching centers protected in facilities classified at the secret level or above. Trunk lines would connect to other switches. Subscribers could co-locate or connect remotely to a switch in a variety of ways. The network was to have highly redundant routing, be easily reconfigured, and ensure extremely high reliability and message delivery. Data security was to be enhanced by using both link encryption through military grade (KG-84) encryption hardware and community of interest (COI) end-to-end encryption through Internet Private Line Interface (IPLI) devices. A new multi-level security project (BLACKER) was to be incorporated into DDN in the late 1980's. Until then, each COI was to treat all data transmissions at one system high level. All sites were to receive similar modular hardware/software and interface services. [Ref. 23]

C. DDN, ACTUAL EVOLUTION

The DDN, like most projects, has changed course to deal with the realities of implementation. These changes have made planning a bit difficult for subscribers. As the transmission medium and interfaces are critical to SPLICE success, it has had to remain flexible in the specification of security requirements. The DDN critical IPLI devices were not being developed as fast as originally planned and

the number of subscribers not yet connected was growing. In 1982 DDN was reevaluated and a decision was made to split classified and unclassified communities. The unclassified segment within the continental U.S. was to become MILNET. Less restrictive requirements were applied to this MILNET segment as of non-military grade encryption standards on the trunk and deletion of IPLI devices. This decision allowed rapid expansion of the MILNET portion. The classified segment and overseas portions of the network remained under the previous standards. "Gates" were set up to allow classified data transmission through MILNET in super-encrypted form. Unclassified users would never pass traffic through or into the classified net. Classified/unclassified segments are optimized independently of each other. [Ref. 24: p. 2] Figure 4.1 illustrates the current SPLICE/MILNET topology.

D. DDN ENCRYPTION

In MILNET, commercial grade Data Encryption Standard (DES) devices were chosen to implement trunk link transmission encryption. DES encryption is discussed in greater detail in Chapter VII. While the trunk is so protected, DDN has made DES protection of remote user access lines an option. [Ref. 24: p. 8]

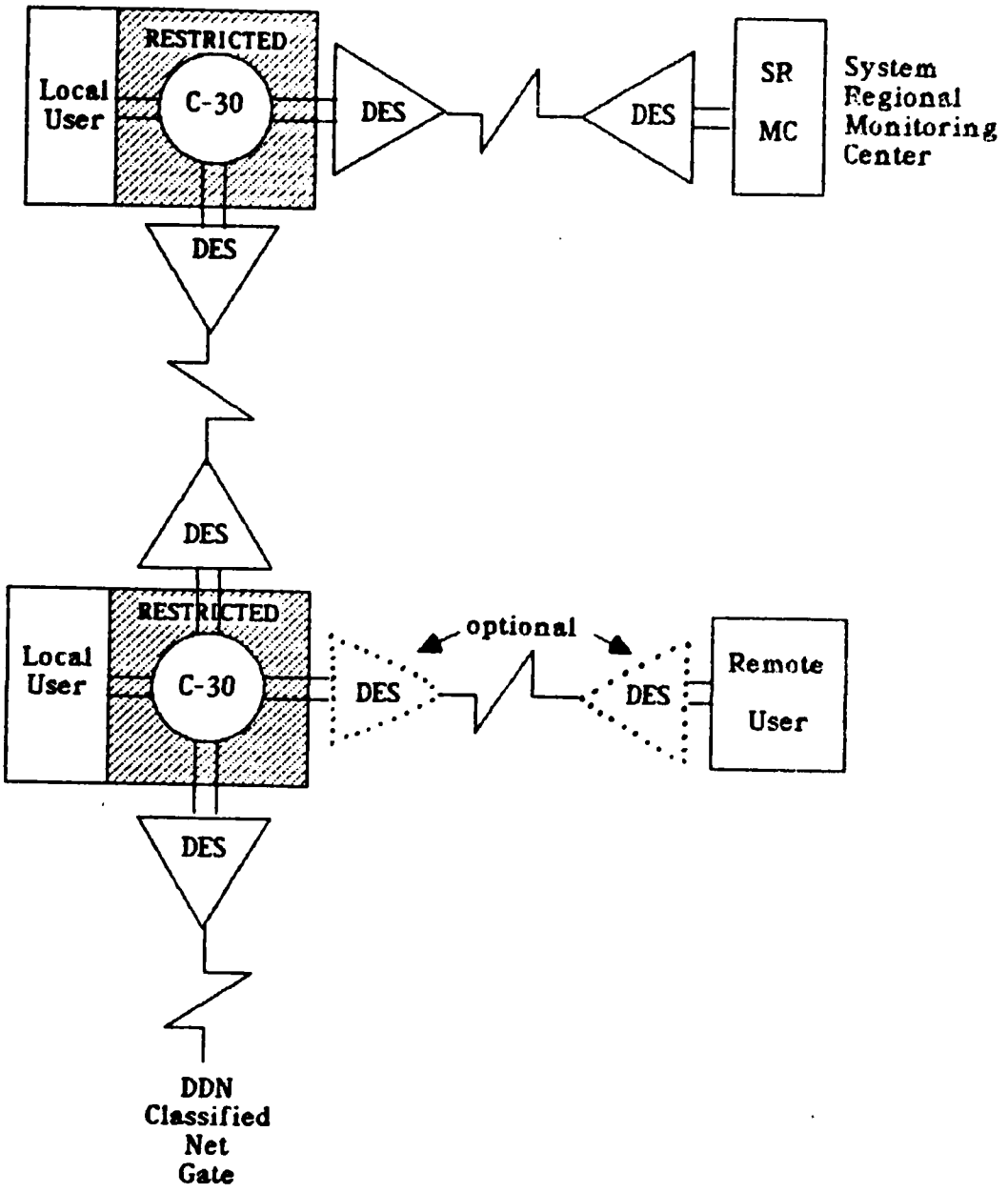


Figure 4.1 [Ref. 24]
Unclassified Segment of DDN

E. PHYSICAL SITE, PERSONNEL

With removal of KG-84 and IPLI provisions in MILNET, switches may now be placed in facilities regarded only as "restricted". This opens a substantial number of locations to switch access at a lower physical security cost. The personnel cleared to work in restricted facilities are not as carefully screened and the risk to both switching equipment and traffic is greater. No restrictions have been placed on configuration placement within a facility.

Since DES hardware at the switch will be tamper protected, data stream security outside the switches can be measured by the physical security afforded the keying material. Restrictions on keying material allow storage in a secured container on site if access is limited to no more than 10 ADP-I critical personnel. [Ref. 24: p. 20] Ten seems a bit high, even for trusted personnel.

F. ELECTRICAL EMMISIONS

DDN equipment will conform to TEMPEST standards [Ref. 24: p. 10]. It is the subscriber's responsibility to protect access lines and organizational equipment. In cases where the nearest DDN switches are a distance away, DES encryption is optional.

G. ACCESS, ROUTING, DELIVERY

DDN documentation clearly states that the subscriber is ultimately responsible for access control.

> "Network facilities in DDN I will not verify... that an individual user (person or process) who attempts to access a subscriber, either directly or through another subscriber, has valid access rights to that subscriber." [Ref. 23]

The DDN requires all subscriber hosts to set access control with userid/password authentication or their equivalent [Ref. 24 p. 17]. Splice access control mechanisms must abide by this. DDN assumes responsibility for proper data routing within a particular unclassified COI by comparing a COI header field in each packet with tables maintained at each switch. As with most physical systems, mistakes or problems can occur. Misdelivery as a result of hardware/software failure, attacks on the DDN segment, or misaddressing has a low probability (5.5×10^{-2}) [Ref. 25: p. 5].

H. THE SPLICE RESPONSE

The decrease in transmission and physical security in the interim DDN MILNET utilized by SPLICE have not met with any increase in security by SPLICE. While performance should remain a key element in SPLICE transactions over DDN, security doesn't deserve a "back burner". IPLI devices were expected to have no significant effect on performance (the equivalent of transfer through an additional switch) [Ref. 9: p. 40]. DES encryption would not be much different.

Without the IPLI devices, SPLICE is not protected by End-to-End encryption. This is balanced by SPLICE non-operability with most other DOD components due to the lack of a "full service" interface because TANDEM software built over X.25 provides SPLICE sites interoperability without full DDN standard protocols [Ref. 23: p. 14]. SPLICE computers will connect with the DDN via Host Front End Processor mode.

V. SECURITY CONTROLS IN SPLICE

A. SPECIFICATION

SPLICE security requirements originally specified in Navy solicitation documents, were followed by Federal Data Corporation in its development of the Security Access System (SAS) and System Monitor (SMON) software. The development of these systems is detailed in a variety of documents [Ref. 27: p. 1].

Primary System requirements included the following or their functional equivalent: [paraphrased from Ref. 26]

- provide restricted access to processes through a user logon requiring a user ID and nondisplayed password;
- *distinctly group users to selected files and processes;* (p. 68)
- record Security Violations in a log showing who, what, when, and where attempted;
- protect all programs and data files to prevent compromise/destruction;
- protect processes or data in primary memory from being accessed/destroyed without authority;
- restrict secondary storage requests to file referenced;
- determine accessor mode by access authorization of ID;
- allow only the central system operator authority to access, establish, modify, or delete user ID's and their authorizations;
- allow storage and maintenance of at least 5000 unique user ID's per site;

- collect user ID in accounting for each process;

- validate terminals and users for transaction level access;

- allow Transaction Processing System control of field level access;

- control file access/use by password;

- require a file to have a password, expiration date, and owner when created. Allow owner right to assign access authorization for file to others and assign, change, or remove passwords for any file owned;

(p. 69)

- provide read only, read/write, execute, read/write/delete, and read/write/execute/delete authorization levels to files;

- restrict deletion to expiration unless first confirming need with Central System Operator/authorized user;

- allow password legibility only to security officer;

- not allow central system operators access to password files;

(p. 70)

- distinquish between at least two levels of process control capability ... central system and user;

(p. 94)

- provide access control by terminal and user to the transaction level;

(p. 98)

- maintain security and integrity of itself and other software components;

- limit configuration access to authorized users;

- process only commands a requestor is authorized to issue;

(p. 101)

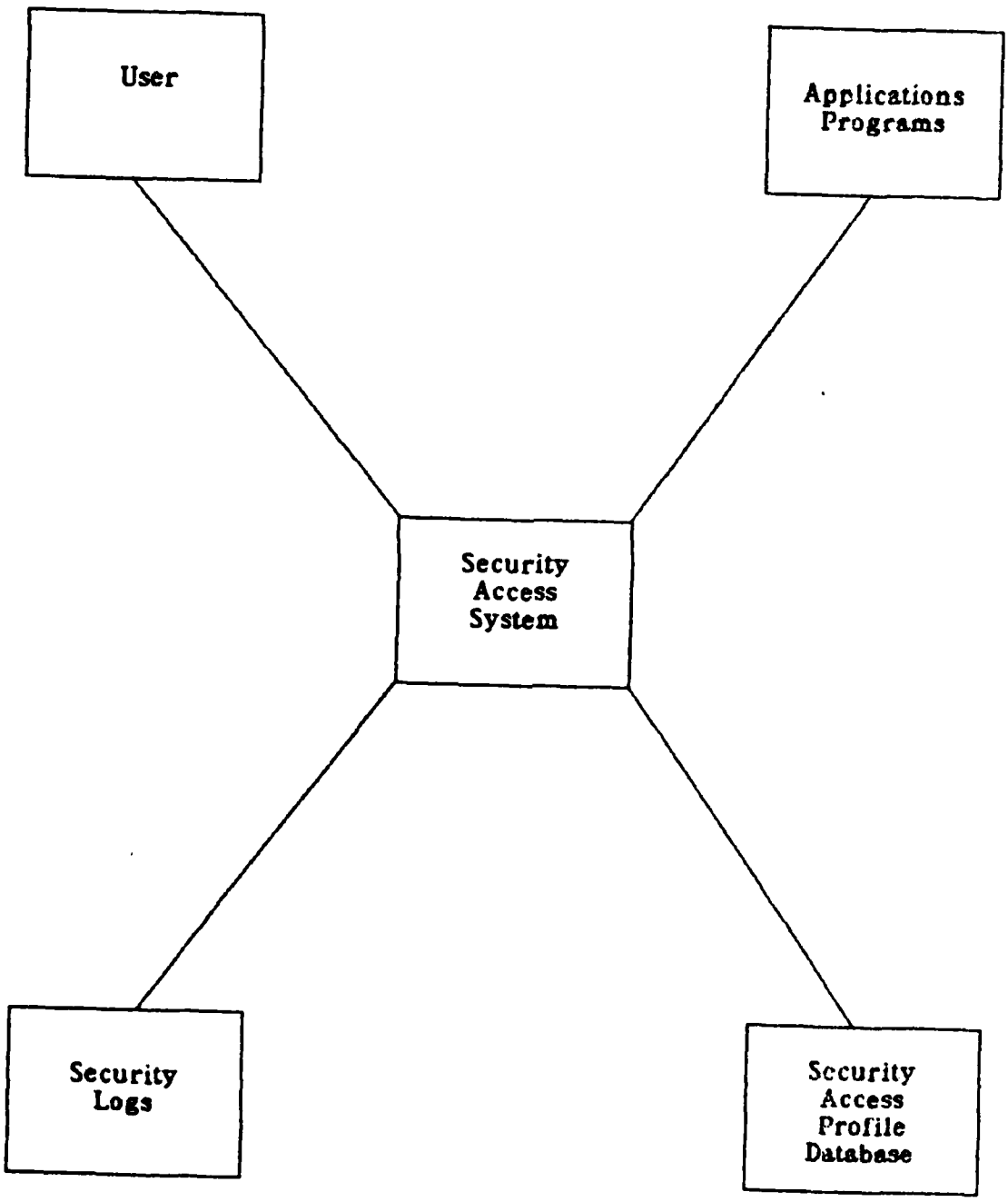
The solicitation document also included reference to use of the Data Encryption Standard (DES) for all proposed products/services to be provided with a cryptographic capability [Ref. 26: p. 43].

These requirements were formalized in the late 1970's. Changes have been made during project development and implementation.

The SAS and SMON subsystems were designed to bring off-the-shelf Tandem operating system software up to access control, routing, and system control requirements of SPLICE. In the transition SPLICE inherited in-place Tandem Software characteristics. Figure 5.1 illustrates elements interacting with SAS.

B. COMPONENT DEVELOPMENT

SPLICE access control is maintained by processes acting on elements of the Security Access System. The SAS was developed under contract by FDC to meet password protection and routing specifications noted above. Through SAS, users are able to logon when authenticated by password and may then perform transactions or call programs as authorized after checks by the Terminal Management Subsystem on SAS databases. SAS overlays the TANDEM GUARDIAN operating system to provide the above features to terminals connected through PATHWAY as well as those having access to the command interpreter. SAS user ID and password structure are



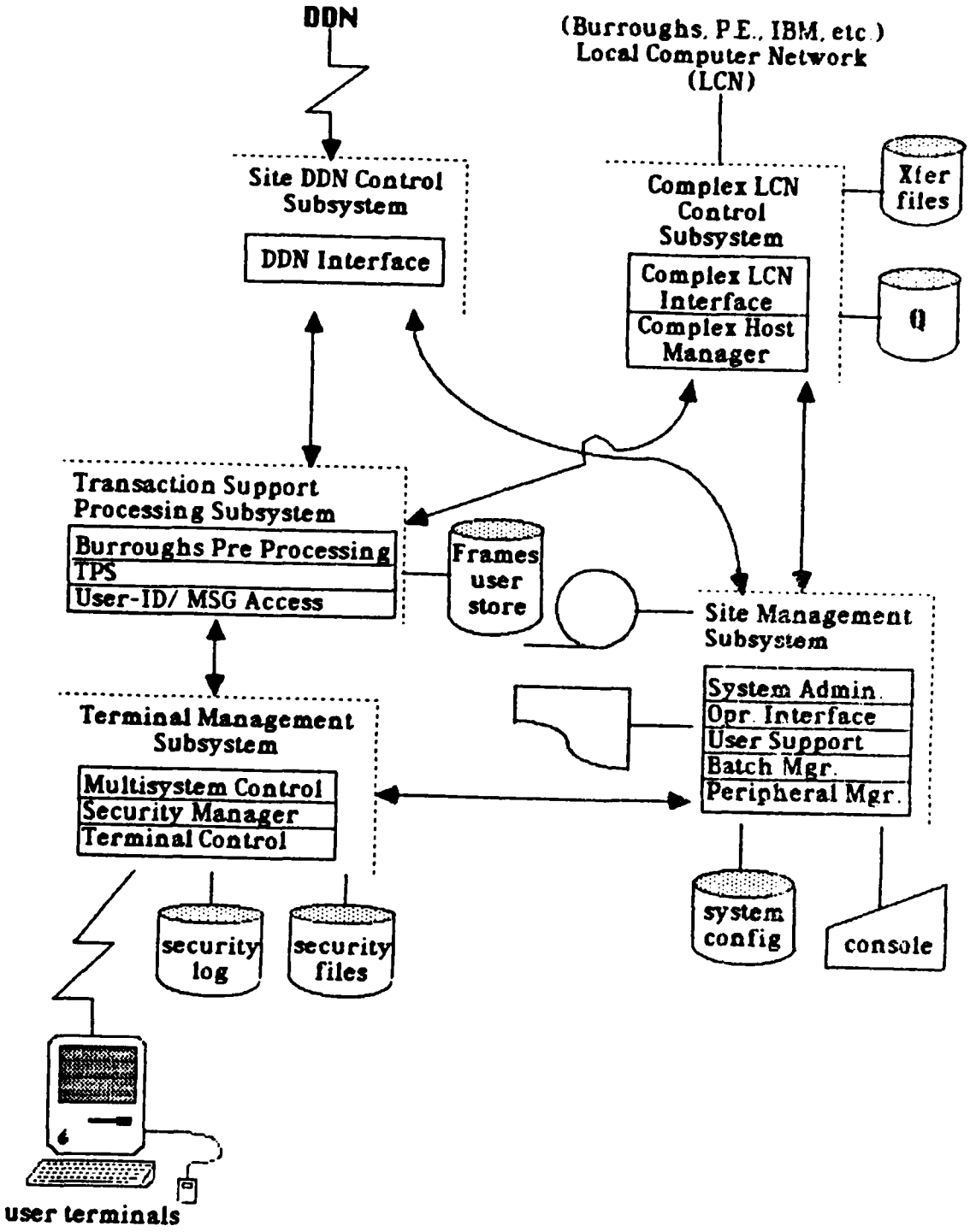
SAS Context Diagram [Ref. 26:p. 4]

Figure 5.1

thus identical to features already in GUARDIAN. SAS specifically authenticates a user, checks both his authority and that of the terminal he utilizes, and optionally routes the user to an authorized destination. SAS contains the Security Access Utility Program (SAUP) for both maintenance of a Security Access Profile database (SAP) and a query capability generating various security reports. SAS operates with the System Monitor (SMON) subsystem for maintenance of security logs, monitoring of user logon/ logoff, and monitoring of system loads and configurations. File Security is maintained by FDC's File Security System with changes possible through File Utility Programs [Ref. 17: p. 9-7] Figure 5.2 depicts logical flow through the Tandem system to DDN and other components.

The first SAS component to be reviewed is the SAP database. SAP is organized into two types of files. Relational Files hold data related to specific users, terminals, programs, transactions, classes of programs/ transactions, and routing. Transformational files are organized in matrix form to allow easy combinatorial operations. [Ref. 27: p. 7]

The user file contains a record for each user and meets SPLICE requirements by listing each user by a unique user ID key with fields for User Logon name, password, authorized program and transaction classes, an optional user initial routing class, an operator identification number for



SPLICE System Logical Flow

Figure 5.2 [Ref. 17: p 3-5]

entering the Terminal Applications Processing system, and activity code data. An additional field exists for user read, write, execute, and purge default file security. The default system will determine other's access to files "owned" by that user. Individual file ownership and security can be changed using the File Utility Program. Access can be restricted to local security officer (super.super), local or remote owner, local or remote group, any local or remote user, local owner only or any local user. [Ref. 27] These restrictions seem to meet SPLICE specifications.

The Terminal File contains a record for each terminal by its PATHWAY filename in ASCII with fields for authorized program and transaction classes [Ref. 27].

A Routing Class File contains records by class specifying choices for initial and TPS routing [Ref. 27].

An Activity Code Description File describes all possible activity codes in the system and a User Activity Table lists up to 65 activities for each user [Ref. 27].

Program and Transaction Description Files are used with Access Files to specify Program and Transaction Classes. Classes specified in Access Files are combined in Matrix Files to determine specific user/terminal combinations.

A Remote Passwords file is maintained with records keyed by User ID and fields for Remote Systems (other SPLICE sites) and remote passwords. Through EXPAND a user in one

site may access authorized programs, transactions, or files in all other SPLICE sites.

The SAUP allows designated security personnel to create and maintain the SAP through use of preformatted screens and selection menus. The SAUP can only be utilized by security and meets SPLICE specifications regarding such a restriction.

Either report or maintenance options can be chosen using function keys. Report options allow the security officer a rapid means of reviewing all program/transaction descriptions, all program/transaction classes for particular users, all activity descriptions, all activities by user, and various combinations of password listings. Maintenance options allow additions, changes, and deletions to SAP files. The preformatted screens both speed maintenance functions and reduce possibility of errors carried into the access control system by allowing only certain combinations of numbers or letters to be placed in each field. Additional controls exist between files to prevent Program or Transaction entities from being deleted from the description file but not the class and to prevent undefined Programs or Transactions from being added to a class.

Registration of new users, terminals, programs, transactions, activities, etc can only be made by security personnel under order from responsible workcenters. Changes

must also be documented by source. By far the biggest problem for each site security officer is maintenance of password features; FDC is responding to requests for assistance here.

C. SAS OPERATIONS

SAS operates through use of a variety of server and requestor structures which will not be discussed in detail here. Users initially enter the system through a LOGON procedure and are authenticated by the password they provide. At this same time the terminal being utilized is identified to the system by a process transparent to the user. An error in LOGON currently results in one of two messages: "USER LOGON ID NOT FOUND IN SYSTEM" or "INVALID PASSWORD" [Ref. 27: p. C-1] While these do provide a degree of friendliness they are not recommended in a System accessable to remote terminals as they allow information to be gained by persons attempting to "crack the system". [Ref. 28] A more generic message requesting repetition of the LOGON process would be superior. Each error in the LOGON attempt results in a write through SMON to system security logs thus meeting original SPLICE specifications for such a feature. Security log notification does not automatically result in a corresponding alarm in the security office or at operator consoles, even on multiple errors or attempts. The system does provide a degree of

protection against computer assisted attempts at cracking the system by allowing only three unsuccessful LOGON attempts and then locking out that terminal for three minutes. This feature is highly recommended by many security experts [Ref. 28: p. 20].

The SAS logon results in a transfer of user/terminal authorization "capability list" data from the SAP database to a Security Access Table created and maintained for the duration of this session (LOGON to LOGOFF). All future session authorization verification checks are made against this table. Access will only be granted when both "(USER ACCESS MATRIX) and (TERMINAL ACCESS MATRIX)" are true for the process requested [Ref. 27: p. 10]. Access results in initial program/transaction routing as provided in routing profiles for that user, or in display of a SELECT menu on the user's terminal. This SELECT menu contains options available for that user.

The SAS system allows checks to be inserted in various SPLICE applications to verify user/terminal authorization during a session at branching points in particular programs. Code must be inserted into the programs at that point directing the process to a TANDEM library routine ALLOWTRANS. This routine checks authorization against SAT and disallows unauthorized activity. All user attempts to request unauthorized processes are written to the security log.

D. LEVEL OF SECURITY PROVIDED

The TANDEM security features implement a "Security Kernel" type architecture on the system. Security appears good if it is assumed the Operating System will not be compromised. An additional problem may result if applications are not coded to incorporate ALLOWTRANS. SPLICE specifications appear to have been met but they may not be sufficient. All transmissions between terminals, processors, and initial DDN switches are open to intercept yielding password and other data. Additionally, security files may be vulnerable in their unencrypted state in the operating system through disk dumps and such.

VI. SURVEY OF AUTHENTICATION

A. REASONS FOR AUTHENTICATION

Authentication is some method for verifying an identity. While authentication has applications in access control to a facility, access control into an on-line computer system is the topic addressed in this chapter. Just as a bank would not wish for strangers to wander through their vault, a computer system manager would not want improperly identified personnel on-line from a terminal or remote site. Not only is the integrity of data in the system at stake, the existence of that data is threatened. An improperly identified user on the system may, by the identity assumed, be allowed access to all data and applications the genuine user was cleared for. Audit trails here would point to the compromised user but not the real culprit. Without reliable user authentication, even strict security access authorization schemes can only limit damage or compromise. Data having value deserves protection.

SPLICE installations require authentication for several reasons. Not all data entry/output points fall within the physical security afforded the central processing site. Users cannot all be observed visually (a form of authentication) because of this remoteness from operating personnel. SPLICE access requests will enter the central

system from both local and remote terminals and by dial-up or dedicated lines from other sites [Ref. 19: p. 9-3]. To ensure viability of access authorization, SPLICE must require authentication.

B. WHAT CAN BE USED TO AUTHENTICATE?

Identify verification techniques use one or more of the following three classes of data:

" 1) something a person knows;

2) something a person has;

3) something a person is."

[Ref. 12: p.66]

Something known includes passwords and background question-and-answer techniques. Something held is exemplified by badges or keys. Something a person is utilizes measurement and matching of some physiological attribute with a standard. SPLICE authentication and commercially available alternatives or possible enhancements will be discussed throughout this chapter.

C. SOMETHING A PERSON KNOWS

Passwords are the best known form of user authentication and are almost universally accepted. Passwords were specified as part of the system user logon procedure in original SPLICE specifications [Ref. 26: p. 68]. With the selection of TANDEM computers and their operating system for SPLICE sites, user identification and password structures

present in GUARDIAN software were applied to meet this specification. The Security Access System (SAS) was developed and added to GUARDIAN. SAS thus provides password authentication over PATHWAY connected terminals at a site. SPLICE specifications specified no password length. Since the GUARDIAN system is configured for up to eight alphanumeric characters this became the defacto standard directed by equipment/software choice. Eight is at the upper end of recommended lengths and provides high security against most password compromises by random manual or computer assisted guessing schemes. Further protection is afforded by a requirement for random generation [Ref. 21].

Most password systems carry with them a high administrative workload resulting from password changes and users forgetting their password and contacting security for help. As users will often be remote from the security office time will be wasted in transporting passwords by person or mail. Changing passwords regularly may also lead users to write down their password rather than rely on memory, potentially compromising the system should passwords be lost or seen by another.

Efforts to make password generation and distribution less of a chore on administrative personnel were not included in the original SPLICE specifications. With installation already taking place this need is now being

addressed. A random password generation program and method to automatically replace passwords in authentication/ authorization tables will take the burden of remote generation and manual entry tasks off the small staffs in site security offices. The ability to automatically address and load the hundreds of letters utilized for password distribution would also be appreciated. Without these aids, a timed replacement of passwords at frequent intervals will be extremely labor intensive and possibly involve others in password system administration increasing the possibility of compromise. As sites each have the capability of storing and maintaining 5000 unique user ID/passwords it can be seen this administrative assistance is desirable.

Vulnerabilities seen in the SPLICE password system principally rest in data access during transmission and storage. The terminal to CPU transmissions and the security files are not encrypted. No portions of the data transmission medium from DDN switches out of DDN into SPLICE are encrypted. Transmissions containing user identification and passwords in combination are thus subject to compromise.

Question-and-answer type authentication systems are both a burden on security and potentially short lived. Background dialogs would have to be developed at user registration. Such background data is more easily determined than a password and the logon delay required by

several exchanges would alienate users. Storage overhead would also result and the registration of remote users would be a problem.

The password system is here to stay even in combination with new technologies and should be supported. Users must be educated to its importance and necessity. Projections that the security features being provided by SAS (under OPNAVINST 5239.1A requirements) will be seen by users as "distasteful" and "inconvenient" [Ref. 17: p.11-9] implies a lack of user understanding of security.

D. SOMETHING A PERSON HAS

The principal devices found in commercial applications from this category read magnetically coded tokens issued to users to authenticate user identity. Possession by the user must be assumed and is the principal shortfall of this entire category. It has therefore been recommended that other authentication techniques be utilized in consonance with it. [Ref. 29: p. 13] The authentication device can be incorporated into the terminal or placed alongside but as yet still appears expensive. While cards may employ many types of coding they are still subject to compromise over time and should be recoded at regular intervals just as passwords should be replaced. SPLICE sites currently use coded cards to open entry door locks at some facilities, but system logon has not been an application.

New "smart cards" are developing which promise a significant increase in data storage for authentication by incorporation of computer chips into the card. Micro Card Technologies, Inc. is selling such cards in bulk at $3.50 to $4.00 [Ref. 30: p. 46]. Such cards could be used for access control, encryption, and even personnel data file information.

E. SOMETHING A PERSON IS

This category uses measurement of various physiological characteristics for identity verification. Techniques showing the most promise include measurements based on fingerprints, hand geometry, signature, speech, and retinal pattern. Most other attributes have been ruled out due to unacceptable delays in measuring/processing or high error rates.

A user first submits to some appropriate measurement test for the attribute sought under observation by security personnel. The measurement device transforms this input into a digital pattern which would then be stored in the security database under a key identifying that user. This "registration" process need not be repeated unless the attribute used is subject to change. Each subsequent access attempt requires that a user first identify himself to the system with the key under which his pattern is stored. Some systems will even search for recognition purposes without a

personnel ID number. The user next utilizes a measurement device to produce a new digital signature. This is compared by the system with the registered pattern; a match opens the channel to access authorization.

This category is not without its problems. In using personal attributes for identity verification there is a difficulty in performing precise, repeatable measurements on the human body [Ref. 29: p. 15]. Because of the measurement problem, many attributes are not feasible alternatives due to a lack of suitable reference points from which to initiate matching. A second problem is lack of variety within a population (Height and weight can be ruled out because they cannot uniquely verify a user identity). Attributes may be so common a device could not be "tuned" to discriminate between users.

Systems must refrain from making 100% positive identification and instead set thresholds for rejection/acceptance based on individual site judgements. If verification settings are too high genuine users will be rejected; this is known as Type I error. If settings are relaxed to decrease Type I errors, the acceptance of falsely identified personnel Type II errors increase. [Ref. 29: p. 16].

One technique to reduce manual intervention by security is the allowance of several access attempts. This has the same effect as changing threshold settings unless the user

is forced to go through a "best two out of three" type scenario. Measurement accuracy usually requires sophisticated devices. While a central operation may well be able to pay for this it would not be justified in a decentralized system with numerous terminals unless data value is extraordinary. A hopeful trend is seen in input devices rapidly dropping in cost. Due to the probability of errors in verification even in accurately measured systems, it appears the best policy will be using this category of authentication only with another method, i.e. passwords.

Automatic speaker verification systems are now on the market. Products now make allowances for noisy background environments and some normal physiological change in the user's voice. Most systems are appearing packaged with automatic speech recognition products requiring significantly greater processing. Both will find wide user acceptance if proven reliable.

During "registration" a user would respond to prompts with a specific set of utterances several times; the computer would establish a pattern for each. During logon the user would receive prompts on screen to repeat a specific subset combination of these. This prompt could be randomly chosen from the security list to prevent ruses such as playing back recordings of the user from being successful. The digital voice prints would be matched and

if successful the user would be passed to access authority areas.

Vendors of current systems for both voice recognition and verification claim reliability factors from 97-99% [Ref. 31: p. 96]. Threshold currently markets a system aimed at Hewlett-Packard PCs and Televideo T950 terminals. Votan is currently marketing multibus units utilizing an IBM PC. Many other manufacturers are entering the marketplace and it is expected that costs will drop rapidly as volume, technological refinement, and competition come into play. With a centrally processed comparison, remote terminals would require little more than a voice input device. Many Security experts expect voice authentication will be brought to market quickly [Ref. 30: p. 46]. This technique deserves close consideration.

A device manufactured by Palmguard Inc., utilizes a user's palmprint for authentication. The model PG-2001 remote terminal can supposedly be used with any host computer and is alledged to reduce type I errors to less than 1% and type II (false accept) to .00025% [Ref. 32: p. 37]. The terminal records palmprints and compares current user prints with those of the registered user. One other notable feature is the recording of print files in the mainframe vs. the terminal; allowing no limit on the number of users registered and lowering device price. The Pg-2001 follows a logon sequence similiar to that previously

discussed. If a match is verified the user's terminal/controller is given an open path into the system. Logs are kept automatically of all attempted accesses.

A system using the retinal eye pattern as its record promises fast, accurate, and secure high level identification of personnel attempting to access a facility or computer system. The Eye Dentification System 7.5 from EyeDentify Inc. is currently marketed in a single standalone unit for $10,000. Registration of up to 1,200 personnel is possible. One key advantage of the system is speed. A user can be registered in approximately 30 seconds. Users receive a personnel identification number (PIN) which they would enter on a touchtone-type key pad integral to the unit. The user would then look into the same double lens eye camera on which registration took place and a low intensity infrared beam would be bounced off the retina. The system takes 320 measurements along a 450° circular scan and creates from this a 40 byte signature. This would be matched with the one taken on registration. Using the PIN, verification takes an average of 1.5 seconds. Without it recognition is still possible without liason from security by trying again. The vendor claims Type I error rates as low as .1% (rejection of user) and Type II rates as low as .0001% [Ref. 33]. Problems related to the eye are also rarely a concern as the retinal pattern is more stable and

unique than a fingerprint. Bloodshot eyes and even most contact lenses reportedly will not interfere. Particular problems can, as with most systems, be tuned out by widening threshold settings for that individual, but security suffers.

If all users operated from but a few areas this system would seem ideal. The need for keys, badges, or easily compromised combinations or passwords is virtually eliminated. SPLICE, unfortunately, is not centralized.

F. DOES SPLICE AUTHENTICATION SUFFER?

Utilizing only password and terminal identifiers is by no means positive identity verification. Even though the password does not appear on screen it is a simple matter (if an insider) to simply watch fellow worker's fingers on the keyboard as they logon. In the past, site security officers have found users sometimes share their passwords with others to simplify work... this problem may still well appear.

While positive verification of user's is difficult, some SPLICE applications may demand it. Without a good verification technique, system audit trials are useless.

VII. ISSUES IN FILE AND TRANSMISSION PROTECTION

A. WHAT IS ENCRYPTION?

Encryption is a technique used to render electronically coded data unintelligible to all but authorized recipients most commonly through use of some transformational algorithm based on a particular data key. Of the various systems for accomplishing this, the Data Encryption Standard (DES) endorsed by the National Bureau of Standards (NBS) is by far the most widely accepted. DES is also mandated for Federal ADP Systems employing encryption for the protection of sensitive yet unclassified data. [Ref. 34]

The DES algorithm is based on 56 bits of a 64 bit key. The remaining bits are used in the error detection mechanism. The key size ensures high level security as it results in "70 quadrillion" possible key combinations. [Ref. 34]. Even with DES in common use efforts to derive the key would be difficult. As even high security may be broken, double encryption would make DES almost impossible to break.

Encryption systems have been designed around the distribution of keys. Data is encrypted utilizing one key and decrypted when necessary utilizing a corresponding key. Users must have the proper keys. Unauthorized personnel must be denied access to keys. The security and operability

of the system thus boils down to adequate key control and distribution.

B. ATTACKS ON DATA

Data is vulnerable to both active and passive attacks in an encrypted system [Ref. 35: p.169]. Even a level of encryption leaves certain vulnerabilities if not effectively employed. The form these attacks take and encryption techniques to counteract them will differ in every part of a system.

Active attacks take the form of transmissions from an attacker with intent to misinform or deny service to legitimate users. Encryption can be used to ensure that an attacker cannot deliver understandable information of his own creation. Encryption alone will not prevent an attacker from recording earlier data streams and injecting them into the line later, so it is a good idea to change keys frequently. In an effort to authenticate transmissions it is also important that messages be assigned sequence numbers by the protocol level they are flowing through. Encryption provides an effective measure of active attack detection when properly utilized and can point security personnel to the point of attack or at least allow the system an opportunity to shut down the line before damage is done. [Ref. 29: p. 23]

Passive attacks take the form of eavesdropping by wiretap or radiation monitoring. Once a signal can be monitored information can be gathered to mount an active attack or achieve the attacker's purpose through other means. Placing a tap between a user terminal and the main processor may lead to compromise of user passwords [Ref. 29: p. 22]. For only a few dollars and a small amount of knowledge most communications lines can be compromised. If an organization does not take steps to protect transmissions, almost any Radio Shack customer can be a potential threat. Where transmission lines leave an activity their integrity ends. Only encryption can be relied on to prevent data compromise over unprotected lines.

C. WHAT SHOULD BE ENCRYPTED?

Data that is of high value or sensitive content should be protected whenever its physical security cannot be guaranteed. Encryption schemes became popular only after numerous high value losses in Electronic Funds Transfer (EFT) systems received wide press coverage in the 1970's. The DES algorithm became a defacto standard in many large banking systems: Bank of America; Chase Manhattan; etc. [Ref. 36: p. 86].

SPLICE exhibits physical vulnerabilities in areas relating to both data transmission and on/off-line storage. Data of value can be found in SPLICE applications involving

the ordering and billing of goods as well as in local applications for contract administration and payroll. Data of a sensitive nature in SPLICE also includes local and remote logon conversations and the actual site security files.

D. WHEN SHOULD ENCRYPTION BE EMPLOYED?

Once the determination has been made that data deserves protection, the physically vulnerable points in the system should be identified. In SPLICE, data transmissions occur between terminals and the TANDEM processors, between processors and output devices, and between processors and memory. In SPLICE connections to other sites or remote terminals, transmissions are made over both dedicated and dial-up lines. In SPLICE connections to DDN, transmissions occur from TANDEM to the nearest DDN switch and between DDN switches. All these links are potential targets for compromise.

The only SPLICE links presently protected by encryption are the DDN links between switches. DDN controls key material. While the costs of encrypting every link system wide may be too much to bear, specific vulnerabilities might be addressed by identifying the most critical. There is a need for this examination in SPLICE. If passwords can be easily deciphered anyone can enter the system and completely circumvent "audit trail" effectiveness. SPLICE should not

rely on DDN or any outside agency to ensure their own data confidentiality.

In a 1981 Security survey of both large and small data processing activities across a broad spectrum of government and business 39% of the respondents reported use of some type of encryption [Ref. 37: p. 42-46]. While such surveys show valuable trends among security conscious users it would probably not be fair to say "39% of all DP organizations" as the majority of non-respondents probably use little security. A 1982 survey of 43 similiar organizations in the Dallas-Fort Worth area showed only a 20% use of some form of data encryption [Ref. 38: p. 25]. Survey results can be of value in pointing to directions being taken by contemporaries but should not be used as the final word for a unique organization.

E. THE COSTS OF ENCRYPTION

Encryption can be implemented in hardware or software depending on organization requirements. Encryption devices are becoming more affordable as the market expands. Initial device expense is not a significant factor in selection of this technique. Numerous commercial products are now affordably priced [Figure 7.1].

> "While NBS DES chips are only $10 or so, the need to generate, distribute, store keys, and integrate encryption into communications protocols, electronic mail, and file systems is non-trivial." [Ref. 39]

Table 7.1 [Ref. 36: p. 84]

DATA-ENCRYPTION SAMPLER

Vendor	Product	Functions
Analytics Communications System	Sherlock ISM $1,995	Authentication; File security; line security; includes DES chip 75 bps to 19.2 Kbps
Com/Tech Syst.	U102 $1,450	Line Security 75 bps to 19.2 Kbps
Datotek	DKG 64,000 $2,000	Line security; includes DES chip up to 64 Kpbs
Industrial Resource Engineering	IRE Scrambler $395	Line security; includes DES chip up to 9600 bps
Racal-Milgo	Datacryptor II $2,100	Line security; includes DES chip 50 to 9600 bps
Sytec	PFX $30,750	Authentication; includes DES chip works with LANS price includes CPU & 50 log-on any LAN speed
Technical Communications	Cipher-X5000 $3,000	Authentication; line security 30 bps to 64 Kbps

Besides the above administrative and design burdens encryption imposes an additional overhead, decreased performance. Software implementations tend to be much slower than hardware and have not gained as wide an acceptance. If a system has been designed to meet user response time requirements without encryption it will probably fail to meet them when encryption is added-on. This is the primary reason encryption should be considered before system development.

Encryption does not guarantee data safety. If a key is lost, the data "protected" by it may be lost forever. It is a good idea to lessen risk of this occurring by using different keys for a backup copy. Key security is a major administrative burden and can lead to operational as well as security problems should it be handled improperly.

Another cost of security is the burden placed on reorganization and recovery. [Ref. 40: p. 419]. If the key is being automatically changed by the system over time a method must be in place to backtrack far enough for restart. Additionally, elements in one area must have a capability to rapidly communicate changes to other affected components.

Key distribution places an administrative burden on the organization and can disrupt operations if not responsive to rapid change should current keys be compromised. It is important that details of distribution be worked out before a system is obtained to ensure that the security office is

aware of the additional responsibilities. Key distribution is usually acomplished utilizing a courier, registered mail, or other secured communications channels [Ref. 19: p. 167].

F. ENCRYPTION METHODS

Two basic encryption methods are in widespread use. In block ciphering, information is encrypted in blocks as it passes through the encryption point. In stream ciphering, a steady stream of encrypted signal is continously transmitted whether a real message has arrived or not. Each method has advantages not found in the other.

Block ciphers are efficient where message segments are easily broken out of traffic. While protecting data well they are still more vulnerable to traffic analysis then the stream cipher as these segments may also be identified by listeners. Frequently changing the key can reduce this. Block ciphers work well with packet switched networks.

Stream ciphers virtually ensure traffic analysis failure by injecting messages into a continous cipher stream produced by the encryption equipment.

Encryption techniques can be employed within a computer system in several ways as reinforcement for security provided by the operating system. System Controlled Cryptographic transformations are made utilizing keys embedded in tamper proof devices controlled by security personnel. Transformations can be performed on every data

segment transfer via DES or other techniques. User Controlled Cryptographic transformations offer individuals more control over their own data by allowing them control of the key. [Ref. 40: p. 414]. This key control could lead to significant problems in cases of loss and may lead to the same vulnerability common to token or password systems should the user write keys down and they fall into the hands of others. SCC transformations make more sense in SPLICE application.

Encryption can be performed at the Link level or End-to-End (E^3). As noted in Chapter III, MILNET is using link encryption between switches. Link encryption would also be appropriate for transmission into and out of dial-up ports. SPLICE should consider its vulnerabilities in connecting to the nearest DDN switch without link encryption. E^3 encryption would ensure SPLICE transmission security across the DDN without reliance only on DDN link security. This had been the reason for IPLI devices. E^3 enciphers data once at the source and leaves it in that condition through to the destination. At no time is sensitive data in plain text even in the DDN switch. Only message addressing/ identifying information need to be left in clear text.

G. PORT PROTECTION

A variety of reasons exist for allowing some users a dial-up capability for access to computer systems. In cases

where use is infrequent the cost of dedicated lines may be prohibitive. This is especially true where the infrequent user is located at great distance. Mobile users such as ships may not have the capability to connect to a single dedicated line every time they are in port. For all these reasons, the connectivity and convenience of dial-up local telephone networks heavily weighs in favor of their use.

Disadvantages of dial-up include less performance and poorer security. Users may be restricted to lower performance modems. Line quality cannot be controlled. Security suffers by a reduced capability for authenticating users leading to potential connections with unauthorized equipment.

Administrative techniques to protect dial-up ports have been developed as vulnerabilities come to light. It has been proposed that system access be restricted to previously arranged and justified applications [Ref. 41: p. 38]. Systems should restrict use only to periods when management personnel are present [Ref. 42: p. 86]. During nonworking hours ports should be physically disconnected from incoming lines. [Ref. 43: p. 34]. Systems should restrict dissemination of dial-port numbers to those with a need-to-know and not use numbers which appear as significant gaps in organizational telephone directories [Ref. 28: p. 27]. Finally management should restrict applications to those of a non-sensitive nature.

Other dial-up protection techniques deal with the interface seen by remote users or their equipment. Dial-up ports should not provide any indication of their computer connections. Organizational logos and user prompts should be avoided where possible. It has been recommended that the line protocols utilized be at a higher level then ASCII asynchronous, leaving personnel computers and dumb terminals at a disadvantage [Ref. 28: p.27]. The system should automatically shut down any line left open without activity for the last "N" minutes [Ref. 43: p.34]. Error messages to a user should not reveal information attackers might use to their advantage [Ref. 42: p. 87]. Terminals should be given some method for identifying themselves transparent to the user (the IBM SDLC protocol for example allows transmission of a "built-in" identifier, a two-byte device type and a two-byte unique identifier) [Ref. 42: p.87]. The activity can additionally employ encryption or dial-back devices.

Dial-back devices are employed to accept incoming calls, authenticate the user, close the connection, and dial-back to a predetermined number for the user seeking access. The advantage of such devices lies in limiting the potential penetrator to the user site or at least to his published phone number. Dial-back additionally eliminates all chances for direct dial-in access on the request line. One other

potential problem known as "drop-off add-on", occurring when an authorized user leaves an open line and other parties come into the system, is also eliminated [Ref. 41: p. 86]. Examples of dial-up port protection devices are in Figure 7.2.

The principal disadvantage of dial-back devices lies in the inconvenience in delay of session initiation. DOD telephone systems are notoriously inadequate at many installations and once a connection is broken it make take several attempts to reintiate. Establishing a direct dedicated number at the user end must be required if shipboard connections with dial-back are to be accepted.

SPLICE plans for dial-up ports are restricted to shipboard logistics in the SNAP I/II program. These users will be given connection capabilities via dial-up from their serving port (i.e. NS Mayport) using 3270 emulation protocols. [Ref. 19: p. 8-3]. The protection features utilized in the past for such connections to UADPS-SP applications have been limited to password protection features in the operating system. It is recommended that encryption or dial-back devices be installed. Ships have been allowed to place orders through past connections in addition to the originally authorized query capabilities. It would seem that this capability needs protection.

TABLE 7.2 [Ref. 36: p. 86]

DIALUP-PORT PROTECTION DEVICES

Vendor	Product	Lines Supported
Digital Pathways	Defender II Model 48	Up to 48 lines
	$10,000	
Penril Datacom	Auto-Data 300/1200S	1 line
	$750	
Wall Data	Interguard	Up to 16 lines
	$6,400	

VIII. CONCLUSIONS/RECOMMENDATIONS

A. CONCLUSIONS

SPLICE is being implemented in a climate of both changing user applications and changing technology. Both the Fleet Material Support Office designed and local unique applications should be carefully examined before SPLICE is utilized for processing or data transfer to ensure that their security requirements are being met. The changing technology can be used to improve the security of a site or break it down. The direction taken will depend on which party places this technology in use first. As the world becomes more computer literate the possibility of dishonest personnel gaining the skills necessary for system compromise grows. If SPLICE is to process and transmit sensitive data it requires protection commensurate with its value.

As we have seen from the review of SAS, SPLICE has come a long way toward improving data security and integrity. The system has been developed and is in the implementation process at several sites. The basic design meets Solicitation Functional Requirements and it has been my experience from field interviews that the vendor, FDC, is supporting user requests for changes made thus far. The custom nature of the SAS software and use of Tandem developed high order language (TAL) in its constructs puts

the responsibility for updates squarely on the vendor. The result of that design choice is not clear; future support remains to be seen. The real test of the system will come when sites begin utilizing the DDN and other links for intersite communications.

It is my opinion, after weighing both advantages and disadvantages of various authentication techniques, that passwords alone should not be relied on. The inclusion of terminal authentication is of great benefit in further limiting vulnerability, especially since program and transaction access can be limited by terminal. A major area of concern left unsecured is a combination passive/active attack on the system possible due to both in-site and between-site unprotected data streams. Both user password and terminal identifier are still being passed in the clear.

Data transmissions between local and remote elements are subject to the same vulnerability found in the authentication area. Data could be analyzed/modified/destroyed without detection. Although encryption suffers from many administrative disadvantages and a slight performance loss it appears warranted here.

Dial-up ports appear to be the only economical method of access for SNAP shipboard systems available now. SPLICE is risking disaster if ports are left unprotected by only the password provisions. The major problem area here appears to

be selection of an appropriate product and establishment of proper administrative safeguards as noted in Chapter VI.

Finally, SPLICE safeguards cannot be analyzed for cost effectiveness without proper Risk Assessments. This area requires more attention and it appears to warrant more central direction; each activity can potentially re-invent the wheel without it.

B. RECOMMENDATIONS

The greatest problem encountered during research was difficulty in locating measures of data value on which to build safeguard selection criteria. The Risk Assessment completed in 1980 was of little use here. It is highly recommended that FMSO develop some set procedures and a possible software tool on which individual site security officers may base their Risk Assessments.

During my review of current literature regarding various authentication techniques and specific products available I found little in the way of comparative data. Ref 29, as far back as 1980 advocated a study of the various security products available for user authentication with rating scales based on that number where adjustments made TYPE I/II errors equal possibilities. I recommend that the Computer Security Center undertake such a study and then place results in their Evaluated Products List data.

I believe that SPLICE data for accounting/payroll/contracts/etc. is of sufficient value to warrant transmission protection by encryption. I also see the value in use of dial-up ports for SNAP users and propose that these ports be protected by dial-back devices as well. Only a system wide review of SPLICE data security requirements will suffice in the actual cost justification process for these features. Plans to complete this assessment and acquire these devices must be started now.

User authentication techniques other then passwords still carry hefty pricetags and probably cannot be justified now in SPLICE. I recommend that a close watch be maintained in this area for new product developments.

APPENDIX A

ABBREVIATIONS

ADP	Automatic Data Processing
ARPANET	Advanced Research Projects Agency Network
AUTODIN II	Automatic Digital Network
COI	Community of Interest
DAAS	Defense Automatic Addressing System
DDN	Defense Data Network
DES	Data Encryption Standard
DLANET	Defense Logistics Agency Network
DOD	Department of Defense
E^3	End-to-End Encryption
FDC	Federal Data Corporation
ICPNET	Inventory Control Point Network
IP	Internet Protocol
IPLI	Internet Private Line Interface
NAVSUP	Naval Supply Systems Command
NBS	National Bureau of Standards
PIN	Personal Identification Number
SAP	Security Access Profile
SAS	Security Access System
SAUP	Security Access Utility Program
SMON	System Monitor System

SPLICE	-------	Stock Point Logistics Integrated Communications Environment
TAL	----------	Tandem Language
TCP	----------	Transmission Control Protocol
UADPS-SP	-----	Uniform Automatic Data Processing System Stock Points

LIST OF REFERENCES

1. Office of Management and Budget, Circular No. A-71, Transmittal Memorandum No. 1, Security of Federal Automated Information Systems, 27 July 1978.

2. OPNAVINST 5239.1A, Subject: Department of the Navy Automated Data Processing Security Program, 03 August 1982.

3. Campbell, R.P., "We Don't Know How to Ask for Security", Government Computer News Vol.3, No.6, June 1984.

4. Bloom, R., "Computers Don't Commit Crime, People Do", Data Management, Vol 21, # 7, pp. 14-17, July 1983.

5. Courtney, R.H., "Computer Security Goals of the DOD-Another Opinion", Computer Security Journal, Vol III, # 1, pp. 61-64, Summer 1984.

6. "Report on Computer Seurity Released", Gov't Computer News, Vol 3, No 6, June 1984.

7. Harris, N.L., "Rigid Administrative Procedures Prevent Computer Security Failure", Data Management, Vol 22, # 12, pp. 13-16, Dec. 1984.

8. Parker, D.B., Computer Security Management, Reston Publishing Company, Inc, 1981.

9. Faurer, L.D., "Information Protection in the Federal and Private Sectors", Computer Security Journal, Vol II, # 2, pp. 89-96, Fall/Winter 1983.

10. Zimmerman, J.S., "The Human Side of Computer Security" Computer Security Journal, Vol III, # 1, pp. 7-20, Summer 1984.

11. Faurer, L.D., "Computer Security Goals of the Department of Defense", Computer Security Journal, Vol. III, # 1, pp. 55-60, Summer 1984.

12. Crowder, S.K., and Adams, J.M., Proposal For Stock Point Logistics Integrated Communications Environment (SPLICE) Local Area Network Risk Management Masters Thesis, Naval Postgraduate School, Monterey, CA., December 1982.

13. Naval Postgraduate School, Monterey, CA., NPS-54-83-015, A Distributed Operating System Design and Dictionary/ Directory for the Stock Point Logistics Integrated Communications Environment, Schneidewind, N.F., and Dolk, D.R., p. 45, November 1983.

14. Silverman, M.E., "Selling Security to Senior Management, DP Personnel, and Users", Computer Security Journal, Vol II, # 2, pp. 7-18, Fall/Winter 1983.

15. Wallach, G.T., "Controls Prevent Computer Negligence and Fraud", Journal of Systems Management, Vol 34, No 5, p. 30, May 1983.

16. Francella, K., "Multiple Controls Combat Computer Crime", Data Management, Vol 21, # 7, p. 21, July 1983.

17. Naval Supply Systems Command, SPLICE Acquisition and Implementation Strategy, 1 July 1984.

18. Naval Supply Systems Command (NAVSUP 041), UADPS-SP SPLICE Requirements Statement (RS), 15 June 1984.

19. Naval Supply Systems Command, Stock Point Logistics Integrated Communications Environment (SPLICE), Data Communications Plan (DCP), Draft, 23 July 1984.

20. Naval Supply Systems Command, Stock Point Logistics Integrated Communications Environment (SPLICE) Security and Risk Assessment Plan, 01 November 1980.

21. Defense Communication Agency, Defense Data Network Subscriber Interface Guide, November 1983.

22. Under Secretary of Defense (R & D) Unclassified Memorandum, Subject: DDN Implementation, 10 March 1983.

23. Defence Communications Agency, Defense Data Network Program Plan, January 1982, (Revised May 1982).

24. Defense Communications Agency, Defense Data Network Subscriber Security Guide, November 1983.

25. Defense Communications Agency, Defense Data Network System Description, January 1984.

26. Federal Data Corporation, Security Access System User's Manual, Rev 1.0, March 1984.

27. Naval Supply Systems Command, Solicitation Document N66032-82-R-0007, Acquisition of Hardware, Software and Services to Support the Stock Point Logistics Integrated Communications Environment (SPLICE) Project at 62 Navy Stock Point Sites, 01 March 1982.

28. Wood, C.C., "Countering Unauthorized Systems Access", Journal of Systems Management, Vol 35, No 4, p. 26, April 1984.

29. U.S. Department of Commerce, National Bureau of Standards, NBS, FIPS PUB 83, Guidelines on User Authentication Techniques for Computer Network Access Control, Sep. 1980.

30. Walden, J., "Cracking Down on Micro Crime", Business Computer Systems pp. 40-59, October 1984.

31. Bridges, A., "Speech Recognition Systems Emerge For Untapped Market", Computer Technology Review, pp. 91-97, Winter 1983.

32. (Staff) Access Line, "Palmguard", Data Management, Vol 21, # 7, p. 37, July 1983.

33. Eyedentify Inc., The Eye Dentification System 7.5, (marketing brochure), Rev 9/84.

34. U. S. Dept. of Commerce, National Bureau of Standards, FIPS Pub. 46, Data Encryption Standard, January 1977.

35. Voydock, V.L., and Kent, S.T., "Security Mechanisms in High Level Network Protocols", ACM Computing Surveys, Vol 15, # 2, pp. 135-171, June 1983.

36. Seaman, J., "Halting Network Intruders", Computer Decisions, Vol 17, # 2, pp. 82-93, 29 January 1985.

37. Cook, J.R., Eure, J.D., Johnston, M.A., and Mattord, H.J., "DPMA Chapters Speak Out on DP Security", Data Management, Vol 20, # 5, pp. 42-46, May 1982.

38. Guynes, S., Laney, M.G., and Zant, R., "Computer Security Practice", Journal of Systems Management, Vol 34, # 6, p. 22, June 1983.

39. Perry, T. S., amd Wallich, P., "Can Computer Crime Be Stopped", IEEE Spectrum, Vol 21, # 5, pp. 34-45, May 1984.

40. Guides, E., "The Design of a Cryptography Based Secure File System" IEEE Transactions on Software Engineering, Vol SE-6, # 5, September 1980.

41. Waldrop, H.A., "Network Control", Computer Decisions, August 1984.

42. Murray, W.H., "Good Computer Security Practices for Two Areas of Current Concern: Personal Computers and Dial-up Systems", Computer Security Journal, Vol II, # 2 pp. 77-88, Fall/Winter 1983.

43. Holley, C.L., and Reynolds, K., "Audit Concerns in an On-line Distributed Computer Network", Journal of Systems Management, Vol 35, No 6, p. 32, June 1984.

BIBLIOGRAPHY

Carlsen, D.D., and Krebill, D.P., The National Communications Module of the Stock Point Logistics Integrated Communications Environment (SPLICE) Local Area Networks, Master's Thesis, Naval Postgraduate School, Monterey CA., June 1983.

Defense Communications Agency, Defense Data Network Subscriber's Interface Guide, November 1983.

Department of Commerce, National Bureau of Standards, Special Publication 500-33, Subject: Considerations in the Selection of Security Measures for Automatic Data Processing Systems, June 1983.

Dixon, J.E., The Database Management Module of the SPLICE System, Master's Thesis, Naval Postgraduate School, Monterey CA., October 1981.

Federal Data Corporation, System Monitor System User's Manual, Rev 1-0, March 1984.

Inman, K.A. Jr., and Marthouse, R.C., Local Area Computer Network Design Issues For Communications, Master's Thesis, Naval Postgraduate School, Monterey, CA., June 1982.

Knapp, T.J., "Selling Data Security to Upper Management", Data Management, Vol 21, # 7, July 1983.

Lamport, L., "Password Authentication With Insecure Communication", Communications of the ACM, Vol 24, No 11, November 1981.

Landwehr, C.E., "The Best Available Technologies for Computer Security" Computer, Vol 16, # 7, July 1983.

Meyers, R., "CSC Actively Seeking Built-in Computer Security", Goverment Computer News, Vol 3, No 6, June 1984.

Naval Postgraduate School, Monterey CA., NPS-54-82-0003, Functional Design of a Local Area Network for the Stock Point Logistics Integrated Communications Environment, Schneidewind, N.F., December 1982.

Naval Postgraduate School, Monterey, CA., NPS-54-81-14, StockPoint Logistics Integrated Communications Environment (SPLICE) Networking Study, Schneidewind, N.F., October 1981.

Opel, C.E., Network Management of the SPLICE Computer Network, Master's Thesis, Naval Postgraduate School, Monterey, CA., December 1982.

Parker, D.B., "The Many Faces of Data Vulnerability", IEEE Spectrum, Vol 21, # 5, May 1984.

Reinhart, J.H. III, and Arana, R., Database and Terminal Management Specifications in Support of Stock Point Logistics Integrated Communications Environment (SPLICE), Master's Thesis, Naval Postgraduate School, Monterey, CA., June, 1982.

Schneidewind, N.F., Methods for Interconnecting Local Area Networks to Long Distance Networks, Computer Magazine (IEEE), September 1983.

Shanker, K.S., "The Total Computer Security Problem", Advances in Computer System Security, Edited by Rein Zurn, Artech House, Inc., 1981.

Sime, M.E., and Coombs, M.J., Designing for Human-Computer Communication, Academic Press, 1983.

U.S. Dept of Commerce, National Bureau of Standards, NBS Special Publication 500-200, Validation of Hardware Implementation of the Data Encryption Standard, November 1977.

Walker, Steven T., "Department of Defense Data Network", Signal, October 1982.

Wallich, P., "Technology 85-Software" IEEE Spectrum, Vol 22, No 1, January 1985.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943	2
3.	Professor Norman F. Schneidewind Code 54Ss Adminstrative Sciences Department Naval Postgraduate School Monterey, California 93943	1
4.	Professor Norman Lyons Code 54Lb Administrative Sciences Department Naval Postgraduate School Monterey, California 93943	1
5.	LCDR Ronald Nichols Fleet Material Support Office Code 94L Mechanicsburg, PA 77055	1
6.	LCDR Dana Fuller Crude, Naval Supply Systems Command Code 0415A Washington, D.C. 20376	1
7.	Mr. David Brown Security Office NSC Oakland, California 94606	1
8.	LCDR Edward Case 273 Cosky Dr Marina, California 93933	1
9.	LT Robert Wyatt DOD Computer Security Center 9800 Savage Rd FT. Meade, MD 20755	1

10. LT Daniel Arseneault, USN 2
CVIC
USS John F. Kennedy (CV-67)
FPO N.Y., N.Y. 09538-2800

11. Computer Technology Programs 1
Code 37
Naval Postgraduate School
Monterey, CA 93943

END

FILMED

7-85

DTIC